SSA-301
ISA Security Compliance Institute — System Security Assurance –
Maintenance of ISASecure® certification

Version 2.2

February 2018

Revision history

version	date	changes
1.4	2014.02.09	Initial version published to http://www.ISASecure.org
1.6	2015.03.20	Use acronym SDLPA, update EDSA-310 reference, update ISASecure certification version numbering format, clarify wording regarding VIT by supplier in R5 and CRT criteria for no-repeat in R7
2.2	2018.02.05	Align with ANSI/ISA-62443-4-1 and IEC 62443-4-1: SDLA certification no longer has an associated certification level, although some SDLPA and SDA-S validations depend upon certification level; address scalable systems: mention scalable systems in overview clause 1, add terms scalable system, layout, reference layout, reference system, call out changes to certified layouts in 4.2, R4, R9

Contents

Foreword

This is one of a series of documents that defines ISASecure® certification for control systems, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This specification is one of the series of documents that describes requirements for ISASecure System Security Assurance (SSA) certification of systems. A description of the ISASecure program and the current list of documents related to ISASecure SSA as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for maintaining ISASecure® SSA (System Security Assurance) certification for a control system, as the system and the ISASecure SSA criteria evolve over time. This document covers certification situations where:

- a certified system has subsequently been modified; or
- the ISASecure certification criteria have changed; or
- both the system and the certification criteria have changed.

In these cases, an evidence impact assessment may be performed in order to determine whether, and in what manner, evidence from a previous certification may be used as evidence toward a new certification. The requirements in this document address these topics.

A certification is called an *initial* certification if it *does not* take into account the results of a prior certification for the system or for a prior version of the system. The criteria for a system to earn an initial certification are defined in [SSA-300].

In overview, in order to obtain an initial ISASecure SSA certification, a supplier must pass a Security Development Lifecycle Process Assessment (SDLPA) equivalent to that defined under the ISASecure SDLA (Security Development Lifecycle Assurance) development process certification. Specifically, in order for a system product from a supplier to achieve ISASecure SSA certification, either

- the supplier must hold an ISASecure SDLA certification, where the system is within the stated scope of the certified process, for development going forward; or
- the supplier passes an equivalent SDLPA evaluation of their development process as part of the SSA evaluation itself.

A supplier may apply for SSA and SDLA certification in parallel.

ISASecure SSA certification of systems has four additional elements:

- Security development artifacts for systems (SDA-S);
- Functional security assessment for systems (FSA-S);
- Functional security assessment for embedded devices (FSA-E); and
- System robustness testing (SRT).

SDA-S examines the artifacts that are the outputs of the supplier's security development processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. FSA-E examines the security capabilities of any embedded devices that are components of the system, recognizing that in some cases security functionality is provided by other system components. SRT has three major elements - Vulnerability Identification Testing (VIT), Communication Robustness Testing (CRT) and Network Stress Testing (NST). VIT scans all components of a system for the presence of known vulnerabilities. CRT and NST verify that the system adequately maintains essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions) at its network interfaces.

A system submitted for SSA certification is compromised of security zones, and an associated certification level for each zone (1, 2, 3, or 4), which are designated by the supplier. The SDLPA and SDA-S assessments are the same for all certification levels with the exception of allowable residual risk for known

security issues. FSA-S and VIT increase in rigor for levels greater than 1; pass/fail criteria for VIT reference applicable FSA-S requirements. FSA-E and CRT criteria are the same regardless of certification level.

For scalable systems, which are systems which support replication of devices and/or zones in order to scale for small and large installations, tests performed by the certifier as part of FSA or SRT will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will consider all layouts to be evaluated under the certification.

This document specifies when and how the results of a previous certification may be used for certification of a modified system, for a certification to a later version of the ISASecure criteria, or for a certification to a higher level for one or more security zones. It specifies the incremental evaluations that are performed when evidence from a prior certification evaluation does not fully apply to the new certification being sought. To specify this, the document discusses this topic in turn for each of the elements of ISASecure SSA certification listed above.

2 Normative references

NOTE 1 The following document is the overarching technical specification for ISASecure SSA certification.

[SSA-300] *ISCI System Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

NOTE 2 The following document provides the technical evaluation criteria for the System Robustness Testing element of an SSA evaluation.

[SSA-310] *ISCI System Security Assurance – Requirements for system robustness testing,* as specified at http://www.ISASecure.org

[EDSA-310] ISCI Embedded Device Security Assurance - Requirements for embedded device robustness testing

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*, as specified at http://www.ISASecure.org

NOTE 3 The following documents provide the technical evaluation criteria for the Functional Security Assessment elements of an SSA evaluation.

[SSA-311] *ISCI System Security Assurance – Functional security assessment for systems,* as specified at http://www.ISASecure.org

[EDSA-311] *ISCI Embedded Device Security Assurance – Functional security assessment,* as specified at http://www.ISASecure.org

NOTE 4 The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] also provides the technical evaluation criteria for an ISASecure SDLA certification of a supplier's lifecycle development process.

[SSA-312] *ISCI System Security Assurance – Security development artifacts for systems,* as specified at http://www.ISASecure.org

[SDLA-312] *ISCI Security Development and Lifecycle Assurance – Security development lifecycle assessment*, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

3.1.1
artifact
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure development methods are a threat model document, a security requirements document, meeting minutes, internal test results.

3.1.2
allocatable
able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device's architectural context, although not directly provided by the device itself.

3.1.3
capability security level
security level that a component or system can provide when properly configured and integrated

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

3.1.4
certification level
number associated with a particular certification granted, where requirements to achieve that certification increase in rigor for higher levels

NOTE An SSA certification for a particular security zone may be SSA Level 1, 2, 3, or 4. A zone certified to SSA Level *n* meets requirements for capability security level *n* as defined in the standard ANSI/ISA-62443-3-3-2013.

3.1.5
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

NOTE This term is used when a simpler term that indicates the role of a "chartered laboratory" is clearer in a particular context.

3.1.6
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.7
embedded device
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.8
essential function
function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.9
evidence impact assessment
identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.10
industrial automation and control system
collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process

3.1.11
initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

NOTE The first ISASecure SSA certification for a system is considered an initial certification *of that system*, regardless of whether embedded devices that are components of the system are ISASecure EDSA certified.

3.1.12
ISASecure version
the ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure SSA 2.6.1

NOTE An ISASecure version will map to document versions of the ISASecure technical specifications that define the technical criteria for certification.

3.1.13
layout
description of a specific instance of a scalable control system, that lists quantities of zones and resident devices, and internal and external interfaces

3.1.14
reference layout
specific layout for scalable control system, that represents security characteristics found in any layout to be SSA certified, in a manner suitable to support certification testing that provides assurance for all such layouts

NOTE A reference layout may be neither the minimum nor the maximum layout for a scalable system. Its properties are specified in a requirement in [SSA-300]. In overview, the reference layout for a control system includes all zones, resident devices in these zones, interfaces and protocols present in any layout in scope for a certification.

3.1.15
reference system
physical instance of a control system, that adheres to a reference layout

NOTE A reference system is used for direct testing performed by the SSA certifier.

3.1.16
scalable control system
control system which supports replication of zones and/or devices to support small and large installations

3.1.17
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.18
security zone
grouping of logical or physical assets that share common security requirements

NOTE 1 A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

NOTE 2 This definition and NOTE 1 are from the standard ANSI/ISA-62443-3-3-2013. A zone configuration is part of the system architecture diagram submitted by applicants for ISASecure SSA certification, as required per [SSA-310].

3.1.19
supported
provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality. In particular, supported functionality need not be allocatable to external entities that exist in the environment of the entity under evaluation.

3.1.20
system
control system

NOTE In the ISASecure SSA documentation, this shorter term is used for convenience to refer to a control system product that may fall under the scope of ISASecure SSA certification. Per the definition above, control systems include safety systems.

3.1.21
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CRT	communication robustness testing
CVE	Common Vulnerabilities and Exposures
DCS	distributed control system
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
FSA-S	functional security assessment for systems
IACS	industrial automation and control system
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
NST	network stress testing
PLC	programmable logic controller
SDA-S	security development artifacts for systems
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
SIF	safety instrumented function
SIS	safety instrumented system
SRT	system robustness testing
SSA	system security assurance
SYM	system – maintenance (of certification)
VIT	vulnerability identification testing

4 Overview

In this section we summarize the approach to maintenance of ISASecure SSA certification as a system and the ISASecure SSA certification requirements evolve over time. The intent of the overall approach is to leverage previous certification results wherever possible to achieve cost effectiveness, while maintaining the integrity of the certification result. Sections 5 - 10 provide more detailed requirements for various certification maintenance scenarios.

4.1 SDLPA Certification Element

In order to achieve any ISASecure SSA certification, whether an initial certification or a subsequent certification, the supplier must either:

- at the time the SSA certification is granted, hold an SDLA certification that applies going forward to the system to be certified; or
- pass a Security Development Lifecycle Process Assessment (SDLPA) which is an evaluation of equivalent SDLPA security development lifecycle process criteria, as part of the evaluation for ISASecure SSA certification.

SDLPA is the evaluation of the supplier's documented process. This is distinct from the security development artifact evaluation (SDA-S), which looks at specific artifacts for the candidate system that are outputs from that process, discussed below.

Therefore, ultimately, the capability to obtain further ISASecure SSA certifications throughout the life of a product will depend upon the supplier maintaining adherence to SDLA requirements for their security development lifecycle process as specified in [SDLA-300].

However, once a specific version of a system product has achieved ISASecure SSA certification, it retains this certification regardless of changes in the supplier's development process or the certification status of this process.

4.2 Modified systems

When a particular version of a system achieves, for example, ISASecure SSA 2.6.1 certification, this particular system version retains this specific certification indefinitely. A system vendor is not *required* to update a system certification for every field patch, component update and layout update (for scalable systems) that creates a new version of the system. The decision to certify a later system version is ultimately an optimization of end customer opinion and cost to the supplier. However, the supplier is required to clearly communicate to the marketplace which version of their system meets the ISASecure criteria, and which version of the criteria it meets, as stated in Requirement ISASecure_SY.R2 of [SSA-300].

If a system has achieved certification, and a modified version of that system is submitted for certification to the same ISASecure version and zone certification levels, the supplier may at their option request consideration for the prior certification evidence for any or all of the certification elements SDLPA, SDA-S, FSA-S, FSA-E, and/or SRT. For those elements for which consideration is requested, a well-defined evidence impact assessment is performed that ultimately determines which aspects of the certification evaluation will need to be carried out for the modified system. Given the scope of changes to the system and security development lifecycle process, if such an assessment is determined not to support an update of the evaluation with confidence, the certifier may elect to perform any or all of the evaluation elements in full for the modified system. If an evidence impact assessment is performed and shows that the modifications to the system, its documentation and the supplier security development lifecycle process would not affect the certification results for one or more of these elements, then no certification tests or evaluations will be necessary in order for the modified system to pass that element of certification. In other cases, partial evaluations may be sufficient. The nature of modifications together with the quality of the analysis of the modifications that is required to be submitted by the supplier to the certifier, are the major factors in determining the effort required to obtain a certification for a modified system. However, by policy, CRT and NST are always run in their entirety on a component or network segment, if any aspects of these test results may have been affected. Also, by policy, VIT is always run in its entirety on the modified system.

User documentation changes are evaluated along with changes to the system itself when a modified system is submitted for certification. However, a system that has had only user documentation changes is considered to retain its certification if the system itself has not changed.

Sections 5-7 discuss requirements for certification of modified systems.

4.3 Updated ISASecure criteria

As in the case of system modifications, a system supplier is not required to update a system certification to the latest ISASecure version. Hence, for example, a system certified to ISASecure SSA 2.6.1 is not required to obtain a certification to ISASecure SSA 3.0.0. However, all systems going through certification after ISASecure SSA 3.0.0 becomes available will be certified to that ISASecure SSA version, in accordance with the ISASecure published transition policy.

Consider the case where a system achieved certification under ISASecure SSA 2.6.1, and the system supplier decides to submit this same system version for certification to the new certification version

ISASecure SSA 3.0.0. This certification process will consist of carrying out the defined delta between the two certification versions.

In most cases, both the system version and the ISASecure SSA certification version will have changed. Consider the case where a system achieved certification under ISASecure SSA 2.6.1, and a *modified* system version is submitted for certification to ISASecure SSA 3.0.0. This certification process will be logically equivalent to first certifying the modified system to ISASecure SSA 2.6.1 using the approach described in 4.2, and then carrying out the defined delta between the two certification versions on the modified system.

Section 8 provides requirements for certification to updated ISASecure SSA certification criteria. Section 9 provides requirements for certifications when both the system and the certification criteria have been updated.

4.4 Certification to a higher level

Once a system has achieved certification with each of its security zones at a specified certification level, the system supplier may modify the system or available process evidence as deemed necessary, and then apply for a system certification specifying a higher level certification for one of more zones. As noted in 4.1, the supplier must hold an ISASecure SDLA certification that applies to the system going forward, or undergo SDLPA as part of the system certification. The validations for SDLPA and SDA-S evaluation criteria related to residual risk due to known security issues, differ by certification level.

Any system modifications are assessed to the original certification levels following the approaches outlined in 4.3. Finally, the certifier will evaluate the FSA-S and SDA-S certification criteria by zone that differ from those at the original zone certification level. Section 10 provides requirements for this case.

5 SSA Certification Elements for a Modified System - SDLPA

This section addresses maintenance of certification for the SDLPA element of an SSA system certification. It offers opportunities for leveraging certification effort across products that are not shared by the other SSA certification elements covered in Section 6.

The SDLPA element of an SSA certification examines the existence of a documented SDL (Security Development Lifecycle) process for an organization. The related SDA-S element examines adherence to this process in the development of the candidate system. Maintenance of SDA-S evidence that a modified system has adhered to the SDL process is discussed in later sections. This section discusses maintenance of evidence for the continued existence of a documented security development lifecycle process, when a modified system is submitted for SSA certification.

If a supplier submits multiple systems for certification, it is likely that the SDLPA assessment related to the existence of the SDL process, will be directly applicable to any number of these certifications. A supplier may choose to formalize this leverage by obtaining a separate ISASecure SDLA certification, which certifies the supplier's security development process independent of specific products. A supplier that applies for an initial or subsequent SSA product certification, and holds a separate SDLA process certification that applies to that product, need take no further action to meet the SDLPA element of the SSA system certification. If a supplier does not hold such an ISASecure SDLA process certification, the certifier must revisit the SDLPA element of the SSA evaluation when a modified system is submitted for certification. However the certifier will take into consideration prior ISASecure process audit evidence from any embedded device or system certification previously achieved by the supplier, as stated in [SSA-300] Requirement ISASecure_SY.R5. For SSA certification, this consideration applies whether multiple certifications represent several releases of the same system model, or several different products. The following requirements detail this approach.

The following submission to the SSA certification process by the system supplier supports the certifier in considering the applicability of evidence from prior ISASecure audits of the supplier's security development lifecycle process, toward a later certification.

Requirement ISASecure_SYM.R1 – Submission of analysis of SDLA requirements for SDLPA

If a system supplier does not hold an applicable ISASecure SDLA process certification, they present a modified system for SSA certification where the system previously achieved SSA certification, and they request consideration for the evidence from that prior SDLPA evaluation and/or any other prior ISASecure audits of the supplier's security development lifecycle process, then the supplier SHALL submit the following to the SSA certification process:

- an analysis of the SDLA matrix, that for each numbered requirement and SDLA ID, considering the validation activity in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312], either:
    - States that no additional actions beyond those previously carried out to meet this requirement under prior ISASecure audits of their security development lifecycle process, were required to meet this validation requirement for this SSA certification, or
    - Briefly describes additional actions beyond those previously carried out to meet this requirement, which were carried out to meet this validation requirement for this certification.

NOTE Regardless of whether the system supplier holds an ISASecure SDLA process certification, a submission is always required of an analysis of the SDLA requirements with respect to potential changes to system artifacts that are outputs from this process for a particular modified system presented for certification, per Requirement ISASecure _SYM.R10 below, related to the SDA-S evaluation element. Requirement ISASecure_SYM.R2 adds the requirement to analyze any potential changes related to evidence previously submitted regarding the existence of a documented SDL process, which is the SDLPA evaluation element. For example, the development group for the modified system may have changed its approach to meeting some SSA SDLA process requirements, or the modified system may have been developed by a different development group than previously, so that prior evidence that describes the SDL applicable to this system no longer applies. In either case it is possible that different process approaches and tools are in place, and therefore different evidence of compliance with SDLA process requirements may be needed.

Requirement ISASecure_SYM.R2 – SDLPA certification element for SSA after achieving first certification

A modified system submitted for certification where that system has previously achieved SSA system certification for the same ISASecure version and zone certification levels, SHALL pass the SDLPA element of the certification if either the first two or the third condition below are met:

- the certifier determines that the development process and tools as used in creating the submitted system are the same, equivalent or better than those used in creating the prior system that achieved certification;
- the certifier validates in the context of the submitted system, those requirements which they would judge would require additional supplier actions beyond that previously carried out to meet these SDLPA requirements for the prior certification, and all are assessed as pass;
- the organization that will develop the modified system going forward holds an ISASecure SDLA certification at the time of application for the certification of the modified system, that applies to the system.

The SDLPA report in the first case MAY include only a summary describing the certifier’s conclusion of the first bullet above, a summary of the validations performed, plus a reference to the prior ISASecure audits of the security development process for this organization.

6 SSA Certification Elements for a Modified System - SDA-S, FSA-S, FSA-E, SRT

The requirements in this section cover certifying a modified system, when a previous version of the system has already been certified to the same ISASecure version and zone certification levels. The requirements are structured to address each of the certification elements (SDA-S, FSA-S, FSA-E, SRT) separately. SRT is

addressed by addressing each of its sub elements VIT, CRT, and NST. In Section 7, a summary requirement is stated that incorporates these requirements together with the SDLPA requirements from Section 5.

6.1 Criteria for applying certification evidence from previous system version

The following requirements provide the general criteria under which evidence from prior certifications is considered applicable toward earning certification for a modified system. Specific requirements on how these criteria are evaluated follow in Section 6.2.

Requirement ISASecure_SYM.R3 – SDA-S certification element for a modified system

If a system has been certified, then a modified version of the system SHALL on the basis of that prior evidence pass the SDA-S element of certification for the same ISASecure version and zone certification levels, if:

- the certifier determines that an evidence impact assessment to determine whether the system modifications may have impacted each line item of the SDA-S can be performed with confidence (where a line item is a cell in the [SDLA-312] matrix, in the column applicable to product certifications; and
- the certifier carries out this assessment; and
- the certifier has evaluated at their discretion, any (and possibly all) of the artifacts associated with the potentially impacted SDA-S line items, and given them pass status.

The SDA-S report in this case MAY include only a summary of the evidence impact assessment relative to SDA-S, and the validations performed, plus a reference to the initial SDA–S evaluation for the system. If the certifier judges that such an evidence impact assessment cannot be performed with confidence, the certifier SHALL carry out a full SDA-S evaluation for the system as described in [SSA-312].

The following requirement covers both FSA-S and FSA-E. For FSA-S, it is to be read without the italicized text shown in the brackets. For FSA-E, it is to be read with only the italicized text within the brackets.

Requirement ISASecure_SYM.R4 – FSA-S and FSA-E certification elements for a modified system

If a system has been certified, then a modified version of the system SHALL on the basis of that prior evidence pass the [FSA-S/*FSA-E*] element of certification for [the system, for the same ISASecure version and zone certification levels /*a particular embedded device component of the system*], if:

- the certifier determines that an evidence impact assessment for the prior [FSA-S/*FSA-E*] results for [the system/ *embedded device*] can be performed with confidence; and
- the certifier carries out this assessment and shows that system modifications have either not impacted these results, or may have impacted few [FSA-S line items in [SSA-311*]/ [FSA-E line items in [EDSA-311]*] in a manner isolated from other line items; and
- the certifier has evaluated any potentially impacted [FSA-S/*FSA-E*] line items and given them pass status.

System modifications SHALL be shown to have no impact on results for a line item of the [FSA-S/*FSA-E for a particular embedded device component*] by showing:

- No system or component architecture change, change to the set of layouts to be certified, functionality change or significant new code has been incorporated related to a security feature referenced by the line item of the [FSA-S/FSA-E].

In this case the certification report covering [FSA-S/*FSA-E*] MAY consist of only a summary of the [FSA-S/ *FSA-E*] evidence impact assessment, results for those line items that were evaluated, and a reference to the initial certification report for the [system/*embedded device component*]. If the certifier determines that an [FSA-S/ *FSA-E*] evidence impact assessment cannot be performed with confidence for [the system /*a particular embedded device component*], or that system and component changes related to the [FSA-S/*FSA-E*] are widespread for [the system/*an embedded device component*], then the certifier SHALL perform the full [FSA-S/*FSA-E*] as indicated for the [system/*embedded device*] and a full report SHALL be provided for that certification element.

NOTE It is well understood that security features do not stand alone and are inherently interrelated in providing coherent protection for a system or device. Therefore if there are sufficient changes to security functionality for the system or component embedded devices which it appears may interact, then the full FSA-S and/or FSA-E is likely to be performed on the modified system. This is because an evidence impact assessment attempting to isolate the line items affected by the modifications, will likely need to examine all [FSA-S/*FSA-E*] line items to gain confidence, which will make this assessment essentially equivalent to simply performing a full [FSA-S/*FSA-E*].

Requirement ISASecure_SYM.R5 – Performance of VIT certification element for a modified system

If a system has been certified, and a revised system later presented for certification, VIT SHALL be executed on the modified system such that the test meets the same requirements as for an initial certification, as described in [SSA-310] and [SSA-420]. In some cases it MAY be run by the supplier instead of the chartered laboratory. In particular, if any CRT or NST tests are required for the certification of the revised system per Requirement ISASecure_SYM.R13, then VIT SHALL be performed by the chartered laboratory. If no CRT or NRT tests are required, the chartered laboratory MAY permit the supplier to perform VIT in accordance with the requirements in [SSA-310] and [SSA-420], and to submit the results. The chartered laboratory MAY rerun the test at their discretion.

Requirement ISASecure_SYM.R6 – Requirements on supplier-executed VIT for modified system

If a supplier executes VIT toward certification of a revised system under the conditions in Requirement ISASecure_SYM.R5, this process SHALL meet the following requirements:

- supplier personnel responsible for the VIT SHALL have successfully completed a training class or 1 year of job experience demonstrating proficiency with the VIT tool to be used,
- the supplier SHALL run the test with a policy file provided by the chartered laboratory,
- the chartered laboratory SHALL witness execution of the VIT by the supplier, including starting the test, saving the report file, and signing of the report. This witnessing MAY be achieved remotely.
- the supplier SHALL submit as evidence of VIT:
    - documentation of the tested system configuration, that contains the same information the chartered laboratory would record if they performed the test;
    - the policy file used to run the test;
    - the command line that was executed to run the test; and
    - the full report from the VIT tool
- the VIT evidence submitted to the chartered laboratory SHALL be signed by a responsible representative of the supplier.

Requirement ISASecure_SYM.R7 – CRT certification element for a modified system

If a system has been certified, then a modified version of the system SHALL on the basis of that prior evidence pass the CRT element of certification if:

- the certifier determines that an evidence impact assessment for CRT results can be performed with confidence; and
- the certifier carries out such an assessment and shows that system modifications have not impacted CRT results.

System modifications SHALL be shown to have no impact on CRT results by showing:

- no system or component architectural modifications have been made to any network protocols, essential functions, or their interactions; and
- no significant new code has been incorporated for any network protocol, essential function, or their interactions; and
- no modifications have been made to the network connections along which CRT traffic was transmitted for the previous CRT evaluation; and
- the modified system has no new components, accessible interfaces to components or changes to the network configuration that impact the visibility to components from the external interfaces to the system.

If it is determined per these criteria that no aspects of CRT results have been affected, the certification report covering CRT MAY consist of only a summary of the CRT evidence impact assessment and references to (1) the prior full CRT report for the system and (2) CRT and certification reports for any component embedded devices that are ISASecure EDSA certified. If any of the types of changes in the first three bullets directly above can be determined by the certifier, with confidence, to be isolated to specific system components and network connections, CRT SHALL be run only on those components and over those connections (for all components for which CRT uses that connection) in order to evaluate the modified system for certification. In this case the CRT report SHALL include the CRT evidence impact assessment, the CRT tests run, and references to the previous full CRT reports. If the certifier determines that a CRT evidence impact assessment that would validate applicable changes or isolate them to specific system components and network paths, cannot be performed with confidence, the modified system SHALL undergo the full CRT certification element, for all applicable protocols, in order to achieve certification for this element and a full report SHALL be provided.

The following requirement related to NST parallels that for CRT above.

Requirement ISASecure_SYM.R8 – NST certification element for a modified system

If a system has been certified, then a modified version of the system SHALL on the basis of that prior evidence pass the NST element of certification if:

- the certifier determines that an evidence impact assessment for NST results can be performed with confidence; and
- the certifier carries out such an assessment and shows that system modifications have not impacted NST results.

System modifications SHALL be shown to have no impact on NST results by showing:

- no system or component architectural modifications have been made to any network protocols, essential functions, or their interactions; and

- no significant new code has been incorporated for any network protocol, essential function, or their interactions; and
- no modifications have been made to the network connections along which NST traffic was transmitted for the previous NST evaluation; and
- the modified system has no new components or accessible interfaces to components.

If it is determined per these criteria that no aspects of NST results have been affected, the certification report covering NST MAY consist of only a summary of the NST evidence impact assessment and a reference to the prior full NST report for the system. If any of the types of code changes in the three bullets directly above can be determined by the certifier, with confidence, to be isolated to specific network segments, NST SHALL be run only on those segments in order to evaluate the modified system for certification. In this case the NST report SHALL include the NST evidence impact assessment, the NST tests run, and a reference to the previous full NST report. If the certifier determines that an evidence impact assessment to validate applicable changes or isolate them to specific network segments cannot be performed with confidence, the modified system SHALL undergo the full NST certification element, for all applicable protocols, in order to achieve certification for this element and a full report SHALL be provided.

6.2 Evidence and assessment for criteria

If based upon the criteria in Section 6.1, a system supplier believes that some or all of the evidence used to certify a previous version of a system is applicable toward certification of a modified system, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified system will include supporting evidence to demonstrate that the criteria stated in the requirements of 6.1 are met. This sub section specifies the nature of that supporting evidence and how the certifier carries out an evidence impact assessment relative to the evidence from the prior certification evaluation, based upon the suppliers' supporting evidence regarding system changes.

Requirement ISASecure_SYM.R9 – Submission of system modification data

A system supplier applying for certification for a modified system, MAY request consideration for SDA-S, FSA-S, FSA-E and/or SRT evaluations done on a prior version of the system that achieved certification. If so, the applicant SHALL submit to the certification process:

- a high level description of modifications to the system since the previous certification including bug fixes, new functions, network or firewall configuration changes - for example, release notes from the supplier and from component suppliers, and any changes to the Scope of SSA Certification document that describes layouts covered by the certification;
- a high level analysis of the impacts of these changes by system component;

This analysis shall describe:

- any new accessible interfaces on prior or new components; and
- any third party component that had new CVE reports against it since the prior certification; whether or not addressed by the time of application for certification; and
- any component with a change in third-party supplied sub components such as:
    - An OS service pack update; or
    - A new database version.
- a high level summary of any changes to user documentation related to system security.

Requirement ISASecure_SYM.R10 – Submission of analysis of system modifications

If a system supplier has submitted evidence per Requirement ISASecure_SYM.R9 – Submission of system modification data, then they SHALL in addition submit the following to the certification process:

- If consideration is requested for prior SDA-S evidence,
    - an analysis of the SDA-S matrix, that for each numbered requirement and SDLA ID, considering the validation activity in the column labeled “Applies for Component or System Certification” in [SDLA-312], either:
    - States that no additional actions beyond those previously carried out to meet this requirement for the prior certification are required to meet this validation requirement for this certification, or
    - Briefly describes additional actions beyond those previously carried out to meet this requirement for the prior certifications, which were carried out to meet this validation requirement for this certification.
- If consideration is requested for prior FSA-S evidence:
    - an analysis of the FSA-S matrix, that notes for each numbered line item in [SSA-311] that applies to a capability security level equal to the certification level for some zone in the system, whether there is any change to the configuration, functionality or code supporting such zones and described by this requirement line item, among the system modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related system modifications reported under Requirement ISASecure_SYM.R9.
- If consideration is requested for prior FSA-E evidence for any embedded device component of the system:
    - an analysis of the FSA-E matrix for the embedded device, that notes for each numbered line item in [EDSA-311] that applies at EDSA certification level 1, whether there is any change to the configuration, functionality or code described by this requirement line item, among the system modifications since the previous system certification. If so, the applicant SHALL provide a mapping to the related system modifications reported under Requirement ISASecure_SYM.R9.
- If consideration is requested for prior CRT or NST evidence:
    - an analysis of the modifications reported under Requirement ISASecure_SYM.R9 that SHALL state which if any of these changes modified the system in a manner listed in Requirement ISASecure_SYM.R7 or ISASecure_SYM.R8, which indicates a potential impact on CRT and/or NST results. The supplier SHALL include rationale for any conclusion that a modification did not occur.

The following requirements describe how the certifier renders a judgment that no certification-relevant changes to a system have occurred. In particular, these requirements enumerate for each element of an ISASecure SSA evaluation, how the certifier makes the decision in an evidence impact assessment, that results of that evaluation element would not be impacted due to the system modifications since a prior certification of the system.

NOTE No requirement is listed below regarding assessment of system modifications impacting VIT. Such an assessment would be inappropriate, since known vulnerabilities change over time even if there is no change to the system. Hence in accordance with Requirement_ISASecure_SYM.R5, full VIT is always run on a modified system.

Requirement ISASecure_SYM.R11 – Determination of no evidence impact for SDA-S line item

When performing an evidence impact assessment for a modified system where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a particular line item of the SDA-S evaluation have occurred if:

- the analysis submitted of the SDA-S matrix as described under Requirement ISASecure_SYM.R10 reports no impact; and
- a certifier review of evidence submitted per Requirement ISASecure_SYM.R9 and Requirement ISASecure_SYM.R10 finds no indication of such an impact after consultation with the system supplier.

Requirement ISASecure_SYM.R12 – Determination of no evidence impact for FSA-S or FSA-E line item

When assessing modifications for a modified system where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a specific FSA-S or FSA-E line item have taken place if:

- the analysis submitted of the FSA-S and FSA-E matrices as described under Requirement ISASecure_SYM.R10 reports no changes to functionality covered by this line item since the last certification; and
- a certifier review of evidence submitted per Requirement ISASecure_SYM.R9 and Requirement ISASecure_SYM.R10 finds no indication of such changes after consultation with the system supplier.

Requirement ISASecure_SYM.R13 – Determination of no evidence impact for CRT or NST

When performing an evidence impact assessment for a modified system where a prior version has been certified, the certifier SHALL determine that no modifications that may impact CRT results or NST results have taken place if:

- the analysis submitted of changes to the system as described under Requirement ISASecure_SYM.R10 reports no changes since the prior certification that indicate potential impact to either one or both of CRT or NST results; and
- a certifier review of the evidence submitted per Requirement ISASecure_SYM.R9 and Requirement ISASecure_SYM.R10 finds no indication of such changes after consultation with the system supplier.

7 Criteria for granting certification to a modified system

The following requirement provides a summary statement of the criteria for granting a certification to a modified system based upon the previously stated requirements in Section 5 and Section 6.

Requirement ISASecure_SYM.R14 – Criteria for granting a certification to a modified system

If system has been certified with security zones $\{z_i\}$ to certification levels $\{n_i\}$, then a modified version of the system SHALL be granted certification to the same zone certification levels and ISASecure SSA version if:

- criteria for passing the SDLPA element of the certification are met per Requirement ISASecure_SYM.R2;
- criteria for passing the SDA-S element of the certification are met per Requirement ISASecure_SYM.R3 and Requirement ISASecure_SYM.R11;
- criteria for passing the FSA-S and FSA-E elements of the certification are met per Requirement ISASecure_SYM.R4 and Requirement ISASecure_SYM.12;

- criteria for passing the VIT element of the certification are met per Requirement ISASecure_SYM.R5 and Requirement ISASecure_SYM.R6;

- criteria for passing the CRT element of the certification are met per Requirement ISASecure_SYM.R7 and Requirement ISASecure_SYM.R13;

- criteria for passing the NST element of the certification are met per Requirement ISASecure_SYM.R8 and Requirement ISASecure_SYM.R13.

Alternatively, for each of the evaluation elements SDLPA, SDA-S, FSA-S, FSA-E, CRT and NST for which the supplier did not request consideration for the prior certification per Requirement ISASecure_SYM.R1 and Requirement ISASecure_SYM.R9, the certifier SHALL evaluate that element under the criteria for initial certification found in [SSA-300].

8 Certification to updated ISASecure criteria

The requirements in this section cover certification of a system that holds a prior certification, to a later version of the ISASecure SSA certification criteria. These requirements suffice in the case that the system itself has not undergone modifications as well. If the system has undergone modifications, see Section 9.

The intent of these requirements is that an evaluation of the delta between versions of the ISASecure criteria is sufficient to support certification to a later version of the criteria.

Requirement ISASecure_SYM.R15 – SDLPA and SDA-S elements for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the SDLPA and SDA-S components of a certification to a later ISASecure SSA version if:

- any new SDLA requirements added in this ISASecure SSA version are assessed as pass under SDLPA for security development process and under SDA-S for the system; and

- any changed SDLA requirements in this ISASecure SSA version are assessed as pass under SDLPA for security development process and under SDA-S for the system.

Requirement ISASecure_SYM.R16 – FSA-S element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the FSA-S component of a certification to a later ISASecure SSA version if:

- any new FSA-S requirements added in this ISASecure SSA version are assessed for the system as either supported or NA; and

- any changed FSA-S requirements in this ISASecure SSA version are assessed for the system as either supported or NA.

Requirement ISASecure_SYM.R17 – FSA-E element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the FSA-E component of a certification to a later ISASecure SSA version if:

- any new applicable FSA-E requirements added in this ISASecure SSA version are assessed for each embedded device component of the system as either supported or allocatable; and

- any changed applicable FSA-E requirements in this ISASecure SSA version are assessed for each embedded device component of the system as either supported or allocatable.

Requirement ISASecure_SYM.R18 – VIT element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the VIT component of a certification to a later ISASecure SSA version if VIT is executed in full against the system and passes per the later ISASecure SSA version.

Requirement ISASecure_SYM.R19 – CRT and NST element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the CRT or NST component, respectively, of a certification to a later ISASecure SSA version if:

- for any new protocols added in this ISASecure SSA version, applicable tests as specified by the later ISASecure CRT or NST specification are carried out and pass; and
- if there is a change in CRT or NST test requirements for a previously certified protocol, then a full CRT for this protocol that meets the requirements of the later ISASecure specification version is carried out and passes.

The following requirement provides a summary statement of the criteria for granting a certification to a later ISASecure SSA version, for a system identical to that which previously achieved ISASecure SSA certification to an earlier ISASecure SSA version. It is based upon the previously stated requirements.

Requirement ISASecure_SYM.R20 – Criteria for granting a certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified with zones $\{z_i\}$ to certification levels $\{n_i\}$ SHALL be granted a certification to a later ISASecure SSA version at these same zone certification levels if:

- certification criteria for passing the SDLPA and SDA-S are met per Requirement ISASecure_SYM.R15.
- certification criteria for passing the FSA-S are met per ISASecure_SYM.R16;
- certification criteria for passing the FSA-E are met per Requirement ISASecure_SYM.R17;
- certification criteria for passing the VIT are met per Requirement ISASecure_SYM.R18; and
- certification criteria for passing the CRT and NST are met per Requirement ISASecure_SYM.R19.

The certification report SHALL cover only the tests and assessments performed for the certification as defined by these requirements.

9 Certification when both system and ISASecure SSA version have changed

It will be a common scenario that a system will have changed by the time a new version of the ISASecure SSA certification criteria is released. Thus it will be useful to be able to certify a modified system to a newer version of ISASecure SSA, without repeating the overall process. The following requirement provides a means to achieve this. It states that requirements are met in this case for both certification of modified systems and certification to later ISASecure SSA versions. These have been defined in previous sections.

Requirement ISASecure_SYM.R21 – Certification of a modified system to a later ISASecure SSA version

For a system that previously received an ISASecure certification, a certifier SHALL grant a certification to a later ISASecure SSA version for a modified system if the criteria in both Requirement ISASecure_SYM.R14 and Requirement ISASecure_SYM.R20 are met.

10 Certification to higher level for a security zone

Once a system has achieved certification ISASecure SSA certification with security zones $\{z_i\}$, to certification levels $\{n_i\}$, the vendor may modify the system or available evidence as deemed necessary, and then apply to change one or more of the levels $\{n_i\}$ to a higher value. The following requirement applies in this situation.

Requirement ISASecure_SYM.R22 – Certification of a system incorporating a higher level security zone

For a system that previously received an ISASecure SSA certification with zones $\{z_i\}$ to certification levels $\{n_i\}$, a certifier SHALL grant a certification with a higher value for one of more of the $n_{i,}$ for this same system or a modified system if:

- the criteria for granting a certification at the original levels $\{n_i\}$ for a modified system are met per Requirement ISASecure_SYM.R14; and
- VIT pass criteria are met for those zones where certification level has increased, at their new higher certification level; and
- the additional FSA-S requirements that apply to a capability security level equal to the new higher certification level for some security zone, that did not apply to a capability security level equal to the prior certification level for that zone, have been assessed as pass; and
- the supplier passes an SDA-S evaluation for those requirements whose validation depends upon capability security level, for those zones where certification level has increased. The capability security level applied for a zone will be equal to its new zone certification level.
- the supplier either holds an ISASecure SDLA certification at the time of granting of the higher level certification, that applies to the system going forward, or passes an ISASecure SDLPA evaluation for those requirements whose validation depends upon capability security level, for those zones where certification level has increased. The capability security level applied for a zone will be equal to its new zone certification level.

In this case the certification report SHALL provide content per Requirement ISASecure_SYM.R14 if this is a modified system, as well as report on the new requirements assessed or validations applied for any new zone certification level(s).

NOTE In SDLA-312 v4.52, the treatment of residual risk related to known security issues depends upon capability security level, and is specified in SDLA requirement SDLA-DM-4.